Electronic Recording Delivery System

System Certification Handbook

DRAFT

VERSION 1

California Department of Justice
CJIS Operations Support Bureau
Electronic Recording Delivery System Program

ELECTRONIC RECORDING DELIVER SYSTEM (ERDS)
SYSTEM CERTIFICATION HANDBOOK
TABLE OF CONTENTS

SECTION 11 Escrow Requirements

SECTION 12 Security Audit Requirements

SECTION 13 Oversight
Local Inspections

SECTION 14 Appendices
Terms and Conditions – System Certification
Sample Resolution
Fee Schedule – PENDING
Disqualifying Offenses
Statutory Authority, Chapter 621
Statutory Authority, Chapter 520
Regulations – PENDING
Baseline Requirements and Technology Standards – Definitions and Terms Included
Forms:
ERDS 0001 - Application for System Certification
ERDS 0006 – Request for Replacement of Certificate or Application Documents
ERDS 0008 - Change of Secure and/or Authorized Access
ERDS 0010 - Application for Withdrawal
ERDS 0011 - Secure and Authorized Access Statement

(Fingerprinting Requirements Document)
BCII 9004 – Request for Exemption from Mandatory Electronic Fingerprint Submission Requirement
BCII 8016 – Sample Request for Live Scan Service
FD 258 – Fingerprint Hard Card

SECTION 1
INTRODUCTION

The Electronic Recording Delivery Act of 2004 authorizes a County Recorder, upon approval by resolution of the board of supervisors and system certification by the Attorney General, to establish an Electronic Recording Delivery System (ERDS) for the delivery and recording of specified digitized or digital electronic records that are an instrument of real estate transactions, subject to specified conditions, including system certification, regulation, and oversight by the Attorney General. (Government Code section 27390-et seq.)

A County Recorder wanting to establish an ERDS for the delivery for recording of specified digitized and digital electronic records must contact the ERDS program and request the Electronic Recording Delivery System Certification Package.

ERDS staff will inform the County Recorder of the availability of the System Certification Package on the Attorney General's website, http://ag.ca.gov/ or will, at the request of the County Recorder, send the package via ground mail.

Within the Attorney General's office, the ERDS Program within the Department of Justice has been established and is responsible for implementing the requirements of the law.

Contact Information:

Department of Justice
Electronic Recording Delivery System Program
P.O. Box 1600526
Sacramento, CA 95816-0526

Telephone: (916) 227-8907
Fax: (916) 227-0595

E-mail address: erds@doj.ca.gov
Website: http://caag.ca.gov/erds

The following procedures establish the requirements to be met for the Certification of an Electronic Recording Delivery System.

By signing the ERDS 0001, Application for System Certification under penalty of perjury, a County Recorder or his/her designee understands and agrees to the Terms and Conditions – System Certification as established by the Attorney General.

SECTION 2
DEFINITIONS

For a detailed explanation of the Definitions used throughout the process of establishing an Electronic Recording Delivery System, refer to the Baseline Requirements and Technology Standards information found in Section 14 – Appendices.

SECTION 3
CONTENTS OF
SYSTEM CERTIFICATION PACKAGE

The System Certification Package will contain the following material:

1. ERDS 0001, Application for System Certification.
2. BCII 8016, Request for Live Scan Service, Preprinted with the ERDS Originating Agency Identifier (ORI), address, mail code, and level of service (for use when submitting fingerprints using the Live Scan Method)
3. FD 258, Fingerprint Hard Card, for use when submitting fingerprints using the Manual Hard Card Method. BCII 9004, Request for Exemption from Mandatory Electronic Fingerprint Submission Requirement must accompany a FD 258, Fingerprint Hard Card. NOTE: Where Live Scan locations are available, hard card submission will not be accepted.
4. ERDS System Certification Handbook containing the following information:
   - Terms and Conditions – System Certification
   - Sample Resolution
   - Escrow Requirements
   - Fee Schedule - PENDING
   - Disqualifying Offenses
   - Statutory Authority – Chapter 621
   - Statutory Authority - Chapter 520
   - Program Regulations - PENDING
   - Baseline Requirements & Technology Standards
   - Forms

SECTION 4
REQUIREMENTS FOR AN
ERDS CERTIFICATION

A County Recorder proceeding with the System Certification process shall comply with the following:

1. Submit a completed ERDS 0001, Application for System Certification to the address on the application. This application must be dated and signed under penalty of perjury attesting to the fact that the applicant has read the materials contained in the System Certification Package. A signed application will indicate that the applicant understands and agrees to the established Terms and Conditions - System Certification.
2. Submit the County's Resolution as approved by the Board of Supervisors.
3. Submit a copy of the Interagency Agreement. (Refer to Fee Schedule).
4. Submit the audit report from an Attorney General approved Computer Security Auditor [Reference Gov. Code 27394 (a)]. The report will contain all elements contained in Section 12, Security Audit Requirements.
5. Submit the name of the Vendor of Software employed by the County Recorder, a copy of the contract and a copy of their Attorney General Vendor of Software Certification.
6. Maintain a list of all personnel/individuals and/or business entities and their classifications designated by the County Recorder as having secure access and/or authorized access to an ERDS as outlined in the Terms and Conditions
7. Submit the name of the Computer Security Auditor employed by the County Recorder, a copy of the contract and a copy of their Attorney General Computer Security Auditor Certificate.
8. Have on file a signed ERDS 0011, Secure and Authorized Access Statement for designated employees. (Refer to Terms and Conditions – System Certification).
9. Meet Escrow Requirements.
10. Submission of fingerprints by one of the following methods:

NOTE: Beginning July 1, 2005 all applicant fingerprint submissions must be transmitted electronically (Follow Step a). In some rare circumstances a FD 258, Fingerprint Hard Card will be accepted if an applicant provides the Department of Justice with a valid reason for not submitting a BCII 8016, Request for Live Scan Service, and the Department of Justice waives the requirement of electronic submission. In those instances, the BCII 9004, Request for Exemption From Mandatory Electronic Fingerprint Submission Requirement must be submitted (Follow Step b).

a. Submitting Fingerprints via a BCII 8016, Request for Live Scan Service (Electronic Submission) may be obtained at most law enforcement agencies. To

obtain the most current locations where live scan fingerprint services are available, an applicant may go on-line to the Attorney General's home page or the Applicant Fingerprint Submission, page both found at http://caag.state.ca.us.

The BCII 8016, Request for Live Scan Service form must be submitted to the law enforcement and/or other agency providing the live scan services. Applicants are encouraged to access the fingerprint web site, www.caag.state.ca.us/fingerprints for fingerprinting locations in their area and to determine if an appointment for fingerprinting is required, if additional fees may be charged for the fingerprint rolling services, and the acceptable method of payment. Fingerprinting fees totaling $57.00 ($32.00 for the state fingerprint submissions and $24.00 for the federal fingerprint submission) will be required. Amounts do not include separate fees that may be charged by an agency for rolling fingerprints

b. Fingerprints Submitted via FD 258, Fingerprint Hard Card (Manual Submission) may be submitted, if fingerprinting has been provided by a certified fingerprint roller. The individual needs to submit their FD 258, Fingerprint Hard Card along with any application for Certification or Approval. The fingerprint card **must** include the certified fingerprint roller's signature and certification number next to their signature. If the quality of the fingerprint image is poor, if data fields are not properly completed, or the signature and certification number of the fingerprint roller are missing, the applicant fingerprint card will be rejected and returned to the applicant.

   In addition, the FD-258, Fingerprint Hard Card must be accompanied by a BCII 9004, Request for Exemption From Mandatory Electronic Fingerprint Submission Requirement. Fingerprinting fees totaling $57.00 ($32.00 for the state fingerprint submissions and $24.00 for the federal fingerprint submission) are required. A **separate** check or money order made payable to the "California Department of Justice-ERDS Program" must accompany any application requesting certification.

c. Individuals residing outside of California and applying for certification in California who cannot be fingerprinted in California must have their fingerprints rolled at a law enforcement agency in their state of residence. A fingerprint-rolling fee may be collected by the law enforcement agency when fingerprints are taken.

   If living outside California, any fingerprints must be submitted via FD 258, Fingerprint Hard Card with the ERDS 0001, Application for System Certification. Fingerprint processing fees totaling $57.00 ($32.00 for the state fingerprint submission and $24.00 for the federal fingerprint submission) are required. A **separate** check or money order made payable to the "California Department of Justice-ERDS Program" must accompany the ERDS 0001 Application for System Certification. The ERDS 0001, Application for System Certification, fingerprints,

and processing fees must be mailed to the Department of Justice at the address indicated on the application.

SECTION 5
SYSTEM CERTIFICATION CRITERIA

The Certification of an ERDS will be based on the following criteria:

1. Receipt of completed ERDS 0001, Application for System Certification.
2. Signature on the ERDS 0001, Application for System Certification attesting to the fact that the system requesting certification meets the Baseline Requirements and Technology Standards and that the applicant agrees to the Terms and Conditions – System Certification.
3. Proof of submission of fingerprints (Copy of BCII 8016, Request for Live Scan Service or FD 258, Fingerprint Hard Card) for individuals designated as having secure access, submission of fingerprinting fees and determination of no disqualifying offenses.
4. Successful Report of Audit findings by a Computer Security Auditor.
5. Proof of Escrow. (Refer to Section 11)
6. Current Interagency Agreement. (Refer to Fee Schedule).
7. Receipt of other required documents. (Refer to Section 4):

    - Resolution
    - Computer Security Auditor contract
    - Vendor Contract
    - List of individuals designated as having secure access and/or authorized access, including their classifications.

SECTION 6
APPLICATION PROCESSING

The ERDS program will respond to the County Recorder with an approval or denial within an estimated timeframe of 90 days of receipt of the application and all associated documents.

One of the following steps will be taken following Department of Justice's review of the ERDS 0001, Application for System Certification.

A. If the application is determined to be incomplete:

An incomplete application is determined by the following criteria

1. Missing/illegible data
2. Supporting documentation not attached
3. Proof of fingerprinting of individuals requesting Secure Access authority not submitted.

ERDS Program will:

Return the application to the applicant with a cover letter explaining the reason for return.

Applicant will:

Have thirty (30) days to respond.
If the applicant does not respond within thirty (30) days, the application shall be considered void.

Note: Within the thirty (30) days, the estimated Department of Justice response timeframe of ninety (90) days is suspended until the application has been resubmitted and received by the ERDS Program.

B. If the application is determined to successfully meet all criteria:

I. Approval of System Certification – System Certification is Non-Transferable

ERDS Program will proceed by:

1. Issuing an Approval Letter
2. Issuing of a Certificate of System Certification

The certificate will reflect the following:

- Date of Issuance
- System Certification Certificate Number
- Name of the County being Certified

- "System Certification is Non-Transferable" will be noted.

C. If the application is determined to be denied:
ERDS Program will proceed by:
1. Issuing a letter of denial, informing the applicant of the reason for denial.

Refer to Section 9 – APPEAL PROCESS

SECTION 7
RENEWAL

The Certificate for System Certification Approval, as issued by the Department of Justice, shall remain in effect within the County Recorder's office for which it is approved without the need for renewal for the life of the ERDS operation in said County. However, in cases where substantive system modifications have been made to an ERDS and/or when notice of system termination, suspension or withdrawal has been issued to the County Recorder by the Department of Justice, re-certification will be required.

SECTION 8
TERMINATE, SUSPEND OR WITHDRAWAL

Termination / Suspend:

For the purpose of ERDS processes, the terms "terminate" and "suspend" are considered interchangeable and are used to designate removal of all privileges of access.

The Attorney General, in close cooperation with County Recorders and public prosecutors, shall monitor the security of an ERDS. In cases of multiple fraudulent transactions the Attorney General may order the suspension of electronic recording delivery systems in any county or multiple counties for a period of up to seven days. The Attorney General may seek an order from the superior court if it is necessary to extend this order.[1] Pursuant to Government Code section 27396(a),

Additional basis for termination and suspension include:

- Non-compliance with the Terms and Conditions – System Certification
- Unsatisfactory audit findings by a Computer Security Auditor
- Non-payment of System Administration Fee. (Refer to Fee Schedule).

Department of Justice shall issue a letter of termination or suspension to the County Recorder notifying that Department of Justice certification is invalid and instructing that the County Recorder immediately cease all operations of an ERDS. A copy of the letter will be provided to the Attorney General and the District Attorney.

Withdrawal from System Certification:

A County Recorder choosing to withdraw their System Certification shall submit the following:

1. ERDS 0010, Application for Withdrawal (Refer to Section 15 Forms).
2. Listing of all employees designated as having secure access and/or authorized access.
3. Listing of associated agencies and/or business entities designated as having secure access and/or authorized access.

Department of Justice will process the request and issue a System Certification Termination letter instructing the County Recorder to cease the ERDS operation and notify all associated agencies and/or business entities of the termination. All System Administrative Fees are non-

[1] Government Code section 27396 (b) (1) provided: The Attorney General, a district attorney, or a city prosecutor may bring an action in the name of the people of the state seeking declaratory or injunctive relief, restitution for damages or economic loss, rescission, or other equitable relief pertaining to any alleged violation of this article or regulations adopted pursuant to this article. Injunctive relief may include, but is not limited to, an order suspending a party from participation in the electronic recording delivery system, on a temporary or permanent basis.

refundable. If, at a later date, the County Recorder chooses to participate in the ERDS program, all initial steps for System Certification will be required.

The Department of Justice will process the No Longer Interested forms on all individuals that had been fingerprinted and were designated as having secure access to an ERDS.

SECTION 9
APPEAL PROCESS

The following steps are available based on either denial of an application or termination/suspension of a certificate.

A. Denial of Application

A denial must be appealed in writing within thirty (30) days of the ERDS program review.

- A program committee will review a request for an Appeal.
- A determination shall be made in writing to the appellant:

  Appeal denied – ERDS staff shall issue a letter informing the appellant.

  Appeal granted – ERDS staff shall issue a letter informing the appellant of the decision to grant the appeal.

B. Termination or Suspension of Certification

A termination or suspension of a certification must be appealed in writing within thirty (30) days of the ERDS program review.

- A program committee shall review a request for an Appeal.
- A determination shall be made in writing to the appellant:

  Appeal denied – ERDS staff shall issue a letter informing the appellant.

  Appeal granted – ERDS staff shall issue a letter informing the appellant of the decision to grant the appeal.

SECTION 10
REQUEST FOR DUPLICATE CERTIFICATE AND/OR COPIES

ERDS 0006, Request for Replacement of Certificate or Application Documents is to be utilized for requesting the documents listed below.

Duplicate Certificate

A County Recorder or his/her designee may request a duplicate Certificate of System Certification for the following reasons. The appropriate fee must accompany the request. (Refer to Fee Schedule)

1. A certificate has been lost, stolen or destroyed.
2. A certificate has been mutilated and is no longer usable.
3. Non-receipt of the original certificate.

Request for Copies

A County Recorder or his/her designee may request copies of any documents designated as public records pertaining to the County Recorder's System Certification Application. The appropriate fee must accompany the request. (Refer to Fee Schedule)

1. Application for System Certification
2. All documents on file

SECTION 11
ESCROW REQUIREMENTS

A Vendor of a County Recorder's ERDS is required to place the ERDS source code and other materials in an approved Escrow Facility. This section establishes the escrow requirements to be met.

Approved Escrow Facility

An Escrow Company approved pursuant to California Code of Regulations, Title 2, beginning with Section 20630.

Escrow Requirements

Electronic recording delivery system software program source code(s) (or hereinafter: "source code") shall be placed in escrow in order to:
(a) Create a record of all versions, including changes or modifications of the source code materials placed in escrow;
(b) Create a record of all applications for access to the source code materials placed in escrow;
(c) Unless otherwise superseded by a contract between a vendor and a county recorder, preserve the necessary source code information to permit the county recorder to continue the use and maintenance of the source code in the event the vendor is unable, or otherwise fails, to provide maintenance.

Electronic Recording Delivery System Program Source Code(s)

"Electronic recording delivery system software program source code(s)" or "source code" consists of the computer program or programs used for the delivery for recording, and return to the party requesting recording, of a digitized electronic record that is an instrument affecting a right, title, or interest in real property or a digital electronic record that is an instrument of reconveyance, substitution of trustee, or assignment of deed of trust and store that digitized or digital electronic record to a storage media for later retrieval and reporting

Vendor Letter of Deposit

Within a timeframe established by the County Recorder of any submission of source code materials by a vendor to an approved escrow facility, the vendor shall acknowledge in writing to the affected County Recorder that they have placed their source code or codes in escrow. The vendor letter of deposit shall include a description of submitted materials sufficient to distinguish them from all other submissions.

The vendor letter of deposit shall state:

(1) That all source code information and materials required by these regulations and other applicable law are included in the deposit.
(2) The name of the approved escrow company and the location of the escrow facility where the source code materials have been placed in escrow. The escrow company, its officers, and directors, shall not hold or exercise any direct or indirect financial interest(s) in the vendor.
(3) The escrow company, its officers, and directors, shall not hold or exercise any direct or indirect financial interest(s) in the vendor.
(4) That the escrow company meets the "requirements for escrow facility" as stated in the Escrow Requirements.

Requirements for Submission

(a) The vendor shall submit the source code, as defined in (c) below, to an approved escrow company for placement in the escrow facility.
(b) For each source code, the materials placed in escrow must be sufficient to maintain every related electronic software program used or intended to be used by any county recorder.
(c) The content of escrow materials should be compiled to allow complete and successful restoration of the ERDS in its production environment with confirmation by a production verification test by qualified personnel using only this content. It should include, but not limited, to the following items:

(1) All software modules-components purchased by the Vendor, and used in building the ERDS.
(2) All licenses and security license keys necessary for successful installation and use of these components.
(3) Full documentation (functional descriptions, interface specifications, instructions for installations and use) for all purchased components from their original manufacturers.
(4) Technical support and warranty information from original manufacturers of the components.
(5) Architectural documentation showing usage of these components in the built ERDS.
(6) All software modules-components (in original source code version) developed by the Vendor and used in building the ERDS.
(7) Full engineering design documentation (diagrams, dictionaries, specifications, unit test scripts) for each developed component.
(8) System architectural design documentation.
(9) Bill of Materials – detailed list of all system components purchased and developed.
(10) Detailed deployment diagrams for production environment and deployment specifications with all "build" and "make" instructions.
(11) Detailed Deployment Plan specifications.
(12) Installation and deployment scripts, configuration files, data definition language scripts, and other instructions necessary for full install of the ERDS.
(13) Data loads used for initiation of production with loading scripts or harnesses.
(14) Production Verification Test (content and expected results).

(15) Copy of all compilers and other deployment tools, if purchased separately from OS software, used with their versions mentioned.
(16) Copy of Operating System "sysgen" instructions used for platform preparations for ERDS deployment at different nodes.
(17) Copy of all OS patches used for platform preparations for ERDS deployment at different nodes.

Updates to Submission

Once used to record a digital or digitized record in any electronic recording delivery system, no source code materials in escrow may be changed or modified. Substantive Modifications as described below requires that a new escrow be established.

Substantive Modifications

The following defines substantive modifications:

(1) To source code –
- Modifications or changes leading to a different functional behavior of ERDS or its part (application)
- Modifications of call signatures in interfaces with purchased components
- Modifications of data structures or structural database objects (add table or add column to a table)
- Any change that require modification of deployment procedures.

(2) To Compilers –
- New version of a compiler is as a substantive modification, if the existing ERDS source code cannot be compiled error free (including warnings) without changes of the source code.

(3) To related software (i.e., libraries or purchased components) –
- Any change in a component or module functionality
- Any change in call signatures of modules or call interfaces

(4) To an operating system –
- Any change or upgrade that relates to security settings or security policies
- Cumulative update to a new service pack level

(5) To a System and/or network devices
- Any changes to the server, workstation and/or network devise hardware/software configuration that impacts the ERDS system.
- Any changes to the network architecture/network design as it pertains to the ERDS.

Elaboration: If an ERDS is designed to be independent of the operating system, only ERDS source code needs to be tested, archived and escrowed. For ERDS application source code, any modification is substantive and must be tested, archived and escrowed.

If an ERDS cannot be designed to be independent of the operating system, then for any operating system, compiler or related software (i.e. libraries), any patch or "hotfix" that corrects one or more vulnerabilities, at least one of which presents "high risk" of system compromise, must be considered "substantive". Such a patch or hotfix must be archived and escrowed to ensure subsequent installations using the original operating system are properly patched.

Deposit Software Modifications into Escrow

(a) Prior to being used to record digital or digitized documents in any electronic recording delivery system, the vendor shall submit all source code changes or modifications into escrow in the same manner and under the same conditions in which the source code materials originally were placed in escrow.

(b) Within a timeframe established by the County Recorder of any submission of changed or modified source code, the vendor shall notify each affected County Recorder that the source code placed in escrow has been changed or modified.

Separation of Interest of Escrow Company with Vendor

A vendor may enter into a written agreement with any escrow company for deposit of each source code. However, the escrow company, its officers, and directors, shall not hold or exercise any direct or indirect financial interest(s) in the vendor.

Requirements for Escrow Facilities

For all electronic recording delivery system software program source code materials each escrow facility shall:
(a) Provide a secure and safe environment in which the humidity, temperature, and air filtration are controlled on a 24-hours-a-day, 7-days-a-week basis. The humidity shall be maintained at 35 percent, plus or minus 2 percent, and the temperature shall be maintained at 65 degrees, plus or minus 3 degrees, Fahrenheit.
(b) Maintain storage away from electrical, magnetic, and other fields which could potentially damage computer media over time.
(c) Have backup capability to maintain the properly secured environment in the event of power outages or natural disasters.
(d) Maintain physical security of the escrow facility with controlled and restricted access to all materials placed in escrow.
(e) Store each source code separately. The source code materials placed in escrow shall be secured in a single container and no other material shall be placed in that container.

Conditions for Access to Materials Placed in Escrow

No access to materials placed in escrow shall occur except as specified in this section.
(a) County Recorder shall provide and maintain a list of people having access to escrow materials. Escrow facility will keep a log of access to the materials stored.
(b) Upon a finding by the Attorney General, county recorder, or district attorney that an escrow facility or escrow company is unable or unwilling to maintain materials in escrow in compliance with these regulations.
(c) The Attorney General may, in furtherance of these regulations, for cause at any time, audit source code materials placed in escrow with an escrow facility for purposes of verifying the contents.
(d) An approved computer security auditor shall have access to any aspect of an electronic recording delivery system, in any form requested to complete their certification of the system. Computer security auditor access shall include, but not be limited to, permission for a thorough examination of source code and the associated approved escrow facility, and necessary authorization and assistance for a penetration study of that system.
(e) The vendor shall be entitled at reasonable times during normal business hours and upon reasonable notice to the escrow company during the term of the escrow agreement to inspect the records of the escrow company pertaining to the escrow agreement.

Integrity of Materials Placed in Escrow

No person having access to the electronic recording delivery system software program source code materials shall interfere with or prevent the escrow representative from monitoring the security and the integrity of the electronic delivery system software program source code materials.

Minimum Terms Required in Agreement

The terms of the agreement between the vendor and the escrow company shall include, but not be limited to, the following elements:

(1) The escrow company, its officers, and directors, do not hold or exercise any direct or indirect financial interest(s) in the vendor.

(2) The vendor, its officer, and directors, do not hold or exercise any direct or indirect financial interest(s) in this escrow company.

(3) No source code placed in escrow shall be changed or modified except as permitted in this chapter.

(4) The time period for the escrow agreement and the date for renewal of the agreement.

(5) A provision that the escrow agreement may be renewed for additional periods.

(6) The due date for renewal shall be no later than 30 days before expiration of the escrow agreement. In the event that the contract is not renewed, the escrow company shall so notify the County Recorder and the Attorney General.

(7) In the event that a vendor does not enter into an escrow arrangement with the escrow company to renew the escrow contract, a County Recorder may negotiate directly with an escrow company for continuance of the escrow, and shall so notify the Attorney General and the vendor in writing within 30 days of the new contract.

(8) In the event that the escrow company is notified by a county recorder of the occurrence of a condition as defined in the escrow agreement allowing access to electronic recording delivery system software program source code materials, the escrow company shall immediately so notify the vendor and the Attorney General and shall provide a copy of the notice from the county recorder.

(9) If the vendor provides an objection in writing within 10 days of the mailing or other service of the notice to the vendor, the escrow company shall not allow access. If the vendor does not object as provided in this subdivision, the escrow company shall permit access to the deposit to the county recorder. For the purposes of this section "object" or "objection" means the delivery by certified mail of an affidavit or declaration to the escrow company by the vendor, with a copy to the county recorder which is demanding access and a copy to the Attorney General. The objection shall state that an access condition either has not occurred or no longer exists. Upon receipt of the objection, the escrow company shall not permit access and shall continue to store the deposit pursuant to the escrow agreement.

(10) A requirement that the Escrow Company submit a copy of every electronic recording delivery system escrow agreement to the County Recorder. The copy shall be submitted by the escrow company within ten days of the date the escrow agreement is signed.

(11) For every submission of an electronic recording delivery system escrow agreement, maintain records which sufficiently identify and describe the materials deposited in escrow to determine compliance with the agreement between the vendor and the escrow company. The escrow company shall not be required to verify the content of the materials submitted.
(12) Notify, in writing, the County Recorder within five days of the initial deposit of electronic recording delivery system source code. The notice shall include the name of the vendor and a list describing each of the items comprising the initial submission.

(13) Notify, in writing, the County Recorder within five days of the termination of any electronic recording delivery system escrow agreement.
(14) Notify, in writing, the Attorney General within five days of the change of the name of the company or the name of the escrow facility, together with the address, phone number, and name of the contact person for the company and/or facility.

Retention of Electronic Recording Delivery System Materials

Records maintained by the escrow company pursuant to these regulations and other applicable law shall be retained for the term of the escrow agreement, and for an additional period of 22 months.

The escrow agreement shall provide for the disposition of the materials placed in escrow.

State Not Liable for Any Costs or Any Other's Actions

Neither the Attorney General nor the State of California shall be responsible for any of the fees claimed by the vendor, election jurisdictions, or the escrow company to establish the escrow contract. Further, neither the Attorney General nor the State of California is a party to the agreement and shall not incur any liability for the actions of the parties involved in this escrow agreement.

SECTION 12
SECURITY AUDIT REQUIREMENTS

Nature and Frequency of Electronic Recording Delivery System Computer Security Audits

An initial audit is required before any Electronic Recording Delivery System may be implemented. An approved Computer Security Auditor shall conduct a security audit of a County Recorders Electronic Recording Delivery System and it's Authorized Submitter(s) for the purpose of validating that the system is reasonably secure from vulnerabilities and unauthorized penetration.

Thereafter, an approved ERDS Computer Security Auditor shall audit the Electronic Recording Delivery System annually for the system to remain certified and an audit shall be performed whenever a substantive modification is made to the Electronic Recording Delivery System.

A computer security audit is a systematic, measurable, technical assessment of how the baseline security requirements required by the Attorney General are applied to an Electronic Recording Delivery System.

Security Audit for Initial Implementation and Substantive Modification

The approved Computer Security Auditor shall conduct an end-to-end security audit of the Electronic Recording Delivery System in accordance with generally accepted information security practices. The approved Computer Security Auditor must document his/her findings during the audit. Information in an audit report shall include, but is not necessarily limited to, the following:

1. Demonstration of the proposed system in its intended operational environment in a test mode. Testing shall include the following:

    - A review of the network configuration showing all network nodes;
    - An inventory of hardware, software and network components comprising the proposed system;
    - An inventory of users and roles assigned to operate the system;
    - Tests showing that digital and digitized documents are neither transmitted nor stored in an unencrypted format anywhere in the system.
    - Tests showing that transmissions only occur between authorized parties. The operational environment must be mapped to identify (a) the servers, workstations and network nodes visible from any ERDS workstation or server, (b) the ERDS workstations and servers visible from any non-ERDS workstation or server, and (c) the users and roles authorized to access ERDS workstations and servers.
    - Remnants of sessions, transmissions and documents are not stored once the user initiating the session and transmitting documents has logged out or been disconnected (either physically or logically).
    - A review of the system design showing all components;

- A review of the source code or selected (or all) software components;
- The test environment must simulate authorized and unauthorized users operating in the roles of county recorder, authorized submitter, agent of authorized submitter, and Internet user.

2. A Description of Deposit Materials showing that the source code has been deposited in Escrow with an Escrow Company approved pursuant to Chapter 6, Division 7, Title 2 of the California Code of Regulation, beginning with Section 20630.

Annual Audit

The County Recorder shall obtain an audit of the Electronic Recording Delivery System at least once every year. An authorized Computer Security Auditor shall perform the audit. The audit shall be conducted in the system's operational environment. Testing shall include the following:

1. A review of the network configuration showing all network nodes;
2. An inventory of hardware, software and network components comprising the proposed system;
3. An inventory of users and roles assigned to operate the system;
4. Tests showing that digital and digitized documents are neither transmitted nor stored in an unencrypted format anywhere in the system.
5. Tests showing that transmissions only occur between authorized parties. The operational environment must be mapped to identify (a) the servers, workstations and network nodes visible from any ERDS workstation or server, (b) the ERDS workstations and servers visible from any non-ERDS workstation or server, and (c) the users and roles authorized to access ERDS workstations and servers.
6. Remnants of sessions, transmissions and documents are not stored once the user initiating the session and transmitting documents has logged out or been disconnected (either physically or logically).
7. Collected audit data correlates to actual activity and all auditable events are collected for audit.
8. Description of Deposit Materials showing that the source code has been deposited in Escrow with an approved Escrow Company.

Audit Report Format

The format for both the Initial and Annual Security Audit shall include, but is not necessarily limited to, the following:

1. A non-technical, business-oriented executive overview.

2. A detailed technical observation/recommendation section.

3. A summary of recommendations in a task-list format.

4. A ranking of the vulnerabilities/weaknesses found during the audit shall be documented utilizing a High, Medium, and Low level-of-risk categorization. Show a correlation of each security vulnerability/weakness to a business risk.

    - High-level vulnerabilities/weaknesses shall be classified as vulnerabilities/weaknesses found to pose a hazardous level of risk to the confidentiality, integrity and/or availability of the data and services provided by the ERDS.
    - Medium-level vulnerabilities/weaknesses shall be classified as vulnerabilities/weaknesses that pose a significant level of risk to the confidentiality, integrity and/or availability of the data and services provided by the ERDS.
    - Low-level vulnerabilities/weaknesses shall be classified as vulnerabilities/weaknesses that do not pose a significant level of risk to the confidentiality, integrity and/or availability of the data and services provided by the ERDS.

5. A diagram depicting results where applicable.

6. A description of the approved Computer Security Auditors methodology.

7. A recommendation for any additional precautions needed to ensure that the system is secure.

The initial security audit report shall be further subdivided and include but will not be limited to the following categories of items:

Audit Categories	System Passes/Fails	Comments, Notes
Safety and security of the system:		
No evidence of breaches during testing		
System performed to specifications		
Physical security measures are adequate to prevent unauthorized access		
User survey conducted with satisfactory results in security confidence		
Vulnerability of the electronic recording delivery system to fraud or penetration:		
All documents entering and exiting the system were encrypted per ERDS requirements		
Mechanisms for encrypting met the ERDS Baseline Requirements and Technology Standards		
Access control measures acted to restrict access based on identity and organizational role		

Authentication correctly identified authorized users		
Satisfactory testing conducted submitting sample documents from location X		
Results of testing of the system's protections against fraud or intrusion, including security testing and penetration studies:		
Penetration testing concluded that the system was not exploitable based on the tests conducted		
Security events were properly recorded and detected in audit logs		
Recommendations for any additional precautions needed to ensure that the system is secure:		
Auditor recommends timing of audits increase/decrease		
Encryption keys should be increased by X		
The organization needs to add to or improve security policies		
Recommendation to add more constrictive controls		
Recommendation to authorize continued use		

System Authorization Decision

Audit findings shall be conveyed to the County Recorder in a written audit report. The initial audit report shall be attached to the ERDS 0001, Application for System Certification, submitted by the County Recorder when applying with Department of Justice for system certification. Thereafter, an annual audit report will be forwarded by the County Recorder to the Department of Justice consistent with the Terms and Conditions-System Certification. There are two types of decisions that can be rendered by the Department of Justice, ERDS Program:

1. Authorization to operate; and

2. Denial of authorization to operate.

Authorization to Operate

If, after assessing the results of the Computer Security Audit, the Department of Justice deems that the Electronic Recording Delivery System has met the Baseline Requirements and Technology Standards established for an Electronic Recording Delivery System with no high-level or medium-level vulnerabilities/weaknesses, an authorization to operate will be issued for the Electronic Recording Delivery System. The authorization will indicate that the Electronic Recording Delivery System is authorized to operate without any significant restrictions or limitations on its operation.

Although not affecting the authorization to operate decision, the County Recorder should take specific actions to reduce or eliminate any low-level vulnerabilities/weaknesses identified by the Computer Security Auditor where it is cost-effective to do so. The County Recorder shall, as the system owner, establish a disciplined and structured process to monitor the effectiveness of the security controls for the Electronic Recording Delivery System.

Denial of Authorization to Operate

If, after assessing the results of the Computer Security Audit, the Attorney General's authorizing official deems that the risk to agency operations, agency assets, or individuals is unacceptable, the authorization to operate the Electronic Recording Delivery System will be denied. The system will not be certified and will not be placed into operation. If the system is currently in operation, all activity shall be halted.

To address the security related deficiencies the County Recorder shall submit a plan of action and milestones to be used by the Department of Justice and Computer Security Auditor to monitor the progress in correcting deficiencies noted during the security audit.

When the security related deficiencies have been addressed and confirmed by the Computer Security Auditor, the County Recorder may request the Department of Justice for reconsideration for authorization to operate and system certification.

The County Recorder shall, as the system owner, establish a disciplined and structured process to monitor the effectiveness of the security controls for the Electronic Recording Delivery System.

Filing Procedures

Upon completion, the final Computer Security Auditors "Security Audit Report", the Attorney General's "System Certification Decision" recommendation and any response to any recommendations shall be transmitted to the board of supervisors, the county recorder, the county district attorney, and the Attorney General. These reports shall be exempt from disclosure under the California Public Records Act (Chapter 3.5 (commencing with Section 6250) of Division 7 of Title1).

SECTION 13
OVERSIGHT

ERDS Local Inspection:

In addition to the annual Computer Security Audit, a County Recorder and any agency or affiliated business entities shall be subject to an ERDS Local Inspection. The purpose of this inspection is to ensure that the requirements, as set forth in these procedures, are being adhered to for the ongoing oversight of an electronic recording delivery system.

An electronic recording delivery system and those individuals having secure access will be subject to a local inspection conducted by an Electronic Recording Delivery System (ERDS) Program Representative of the Department of Justice.

1. Notification of Inspection

Contact will be made by the ERDS program representative to the County Recorder or his/her designee to schedule an on-site inspection of the electronic recording delivery system and all associated processes.

2. County Recorder Office Local Inspection Criteria

An ERDS Program Policy and Security Review form *(Security Review form to be developed)* will be used to document areas of non-compliance and of compliance to all inspection criteria. The ERDS program representative will verify the following:

a. That security testing of the electronic recording delivery system has been conducted.

b. That reports of the computer security auditor are being maintained and the following are referenced:

- Safety and security of the system, including the vulnerability of the electronic recording delivery system to fraud or penetration.
- Results of testing of the system's protections against fraud or intrusion, including security testing and penetration studies.
- Recommendations for any additional precautions needed to ensure that the system is secure.
- That documentation has been maintained in cases where the County Recorder, a computer security auditor, a District Attorney for a county participating in the ERDS, or the Attorney General reasonably believes that an ERDS is vulnerable to fraud or intrusion. Records will show the

steps that the County Recorder took to guard against any compromise of the ERDS.

- That reports and any response to any recommendations are being transmitted to the board of supervisors, the County Recorder, the County District Attorney and the Attorney General.
- That a Computer Security Auditor's name, copy of the Attorney General's certificate and a copy of their contract are on file.
- That a Vendor of Software name, Attorney General certificate, a copy of their contract and their Letter of Deposit to an approved Escrow Facility are on file.

c. That a copy of the County's System Certification is on File.

d. That a copy of the County Board of Supervisors Resolution approving participation in an ERDS is on file.

e. That those personnel within the County Recorders office or an affiliated agency or business entity, have a signed ERDS 0011, Secure and Authorized Access Statement, on file acknowledging an understanding of the requirements of secure and authorized access.

f. That a list of all employees or designated individuals with secure access and/or authorized access at the county or with any agency or business entity associated with said county is being maintained. The list will contain all contact information.

g. That required training in the secure handling, storage and destruction of any recorded documents has been conducted.

h. That notification to the Department of Justice has been made when a County Recorder, an employee of the county or an employee of any associated agency or business entity of the county who have been designated with secure and/or authorized access, have been terminated, left employment or have been removed from the duties of requiring secure access to an ERDS.

3. Associated Agencies or Business Entities Local Inspection Criteria

An ERDS Program Policy and Security Review form *(Security Review form to be developed)* will be used to document areas of non-compliance and of compliance to all inspection criteria. The ERDS program representative will verify the following:

a. That the agency or business entity has a copy of an agreement on file allowing them to submit documents to the County Recorder.

b. That a list of all employees designated by a County Recorder within the agency or business entity associated with said county, as having secure and/or authorized access, is being maintained.

c. That those personnel having access to an ERDS have a signed ERDS 0011, Secure and Authorized Access Statement, on file acknowledging an understanding of the requirements of secure and authorized access.

d. That notification to the County Recorder has been made with a copy being provided to the Department of Justice, when individuals who have been designated with secure access and/or authorized access, have been terminated, left employment or have been removed from the duties of requiring secure access to an ERDS.

e. That the agency or business entity has provided training in the secure handling of documents being entered into an ERDS.

4. Inspection Results

a. The ERDS program representative will discuss the findings of the inspection with the County Recorder or his/her designee.

b. A completed ERDS Program Policy and Security Review form *(Security Review form to be developed)* will be provided to the County Recorder or his/her designee at the completion of the ERDS inspection. The form will identify any out of compliance issue(s) discovered during the inspection.

c. The Policy and Security Review form will be signed and dated by both the County Recorder or his/her designee and the ERDS program representative.

d. In the case where the inspection is conducted at a location other than a County Recorder, a copy of the results will be sent to the County Recorder that the agency or business entity is associated with.

5. Non-compliance Letter

In the case of an inspection resulting in the need for corrective action to a non-compliance issue, the ERDS program representative will:

a. Prepare a letter to the County Recorder, or his/her designee, outlining the area(s) indicated in the Security Review form *(Security Review form to be developed)* that need to be addressed.

b. In the case where the inspection in question is within an agency or entity associated with the County Recorder, the letter of non-compliance will be sent to the agency or entity and a copy sent to the County Recorder.

c. A response date will be indicated on the letter notifying the County Recorder when the Department of Justice should receive their explanation of corrective action.

d. If the Department of Justice does not receive a response of corrective action, the ERDS Representative will initiate a follow-up telephone call to inquire as to the status of the response and allow the agency an additional 2 weeks to respond.

e. If corrective action has not been received by the Department of Justice after the follow-up call has been made and the extension granted, The Attorney General or his/her designee in the ERDS Program shall issue a letter of ERDS Suspension.

f. The ERDS Suspension will remain in effect until which time the issue has been resolved.

g. The responsibility will lie with the County Recorder to notify all of their associates of the suspension.

h. Once the ERDS program receives a response of corrective action, the suspension will be removed and a Compliance Letter will be issued.

6. Compliance Letter

In the case of an audit resulting in an agency deemed in compliance with all laws and regulations, the ERDS program representative will:

a. Prepare a congratulatory letter to the County Recorder, or his/her designee, notifying them of their compliance.

b. If an agency or business entity associated with a said county receives a congratulatory letter from the Department of Justice, a copy will be forwarded to the associated County Recorder notifying them of the successful inspection.

SECTION 14
APPENDICES/FORMS

The Appendices include the following documents:

Terms and Conditions – System Certification
Sample Resolution
Fee Schedule - PENDING
Disqualifying Offenses
Statutory Authority, Chapter 621
Statutory Authority, Chapter 520
Regulations – PENDING
Baseline Requirements and Technology Standards

TERMS AND CONDITIONS- System Certification

The overall responsibility for administering the Terms and Conditions- System Certification rests with the County Recorder. By placing my signature on the ERDS 0001, Application for System Certification, I attest that I have read, understand and agree to the following:

1. That the County Recorder shall take steps to guard against any compromise of the electronic recording delivery system and, if necessary, implement the suspension of an authorized submitter or of the electronic delivery system if the County Recorder believes that the electronic recording delivery system is vulnerable to fraud, intrusion or security breaches and report such occurrences to the Department of Justice.

2. That the County Recorder will ensure the placement of a copy of the operating system, source code, compilers, and all related software associated with the electronic recording delivery system in an approved escrow facility.

3. That the County Recorder will ensure that substantive modifications to an operating system, compilers, related software, or source code are approved by the Attorney General and will ensure that the County Recorder's electronic recording delivery system meets the requirements as set forth in the Baseline Requirements and Technology Standards.

4. That the County Recorder is aware of all ERDS requirements as developed by Department of Justice and establishes appropriate policies and procedures to meet and maintain the ERDS system certification requirements, and determines the need for and to provide appropriate training in to individuals designated by the County Recorder in support of the policies and procedures.

5. That the electronic recording delivery system including all associated personnel/individuals and processes are subject to audit and local inspection.

6. That security testing of the electronic recording delivery system is conducted annually by an approved computer security auditor.

7. That reports of the computer security auditor are maintained in file and kept for a minimum of 2 years.

8. That a copy of the County's System Certification is kept in file and available for audit or inspection.

9. That a copy of the County Board of Supervisors Resolution approving participation in an ERDS is on file.

10. That a ERDS 0011, Secure and Authorized Access Statement, is on file, read and signed by all personnel/individuals designated by the County Recorder as having secure access and/or authorized access to an ERDS.

11. That personnel/individuals designated as having secure access to an ERDS have a fingerprint background clearance record check, to include both California and FBI.

12. That a list of all personnel/individuals designated by the County Recorder as having secure access and/or authorized access is being maintained.

13. That notification shall be made within 72 hours to the Department of Justice when an individual who has been designated as having secure access and/or authorized access either has a change of address or has been terminated and/or suspended, left employment or has been removed from the duties of requiring secure or authorized access to an ERDS. Submit completed ERDS 0008, Change of Secure and/or Authorized Access.

[NOTE: EACH COUNTY'S RESOLUTION MAY BE REVISED TO MEET THEIR NEEDS.]

RESOLUTION OF THE COUNTY OF _____ BOARD OF SUPERVISORS
APPROVING THE COUNTY OF _____ TO ESTABLISH AN
ELECTRONIC RECORDING DELIVERY SYSTEM

WHEREAS, Assembly Bill 578 added to the Government Code, Chapter 6, Section 27390 through 27399 establishing the Electronic Recording Delivery Act (ERDA). Government Code Section 27391(a) authorizes a county recorder, upon approval by resolution of the board of supervisors, to establish an electronic recording delivery system for the delivery for recording specified digitized and digital electronic records upon system certification by the Attorney General.

WHEREAS, Government Code section 27397 (c)(1) authorizes a county recorder to impose a fee in an amount up to and including one dollar ($1) for each Real Property instrument that is recorded by county; and

WHEREAS, Government Code section 27397 (c)(2) authorizes a county recorder to impose a fee upon any vendor seeking approval of software and other services as part of an electronic recording delivery system and upon any person seeking to contract as an authorized submitter; and

WHEREAS, the California Attorney General is responsible for establishing regulations and has been delegated the authority for system certification, regulation and oversight of the Electronic Recording Delivery System, and the County Recorder shall comply with all regulations established by the Attorney General; and

NOW, THEREFORE, BE IT RESOLVED that the County of _____ Board of Supervisors:

- Approves the County Recorder to establish an Electronic Recording Delivery System.

- Appoints the County Registrar-Recorder /County Clerk, or his/her designee, as agent to conduct all negotiations and execute and submit all documents necessary for the establishment of an electronic recording delivery system.

- Approves the County of _____ Registrar-Recorder /County Clerk, or his/her designee, as agent to impose a fee up to and including one dollar($1) for each Real Property instrument that is recorded by the County.

- Approves the County of _____ Registrar-Recorder /County Clerk, or his/her designee, as agent to impose a fee upon any vendor seeking

approval of software and other services as part of an electronic recording delivery system and upon any person seeking to contract as an authorized submitter.

- Approves the County Registrar-Recorder /County Clerk, or his/her designee, as agent to issue payments to the California Attorney General through the Department of Justice for County's proportionate share of the direct cost of regulation and oversight by the Attorney General; and

NOW THEREFORE, BE IT FURTHER RESOLVED, that the County of _____ is:

- Approved to submit an application for Electronic Recording Delivery System Certification to the Department of Justice, and, in doing so will comply with the California Code of Regulations, Title _____, Division _____, Chapter _____, Articles 1 through 4; and

- That the County Registrar-Recorder /County Clerk, or his/her designee or agent shall designate those individuals whom are employees of the County Recorder and/or a business entity associated with a County Recorder and whom the County Recorder designates as having secure access and that those persons entrusted with secure access comply with Government Code Section 27395 (b); and

- That the County Registrar-Recorder/County Clerk, or his/her designee or agent shall notify the Department of Justice if an individual that has been granted secure access no longer requires that authorization so that the Department of Justice can meet the requirements of California Penal Code Section 11105.2(d).

THE FOREGOING RESOLUTION WAS DULY ADOPTED by the Board of Supervisors of the County of _____, State of California, on the _____.
(Day/Month/Year)

APPROVED BY:

_____
Signature of Board of Supervisor, Officer

_____
Signature of County Recorder, Designee

(Revised Version 110305)

Fee Schedule

Process	Fee	Trans Code ASD to assign	Trans Title (for DOJ use only)	Fund
Vendor				
Initial Vendor and Software Certification	TBD			Electronic Recording Authorization Account
Renewal Certification	TBD			Electronic Recording Authorization Account
County				
System Administration Fee	This fee is allocated to each participating county by the total documents recorded and filed as reported to the Office of the Insurance Commissioner, as provided in Government Code section 27296, for the previous year. The formula to determine a county's proportionate cost is set by the total documents recorded and filed per individual participating counties divided by the total documents recorded and filed by all participating counties. The percentage figure obtained for each participating county is applied to the estimated annual costs of the Attorney General to arrive at an individual participating county figure.			Electronic Recording Authorization Account
MISC				
Fingerprint (State) Hard Card & Live Scan	$32.00			Fingerprinting Fee Account
Fingerprint (Fed) Hard Card & Live Scan	$24.00			Fingerprinting Fee Account
Returned Item (DOJ Manual 13230)	$10.00			Electronic Recording Authorization Account
Re-issuance of Certification (lost/destroyed)	$10.00			Electronic Recording Authorization Account
Copies (Admin Bulletin 05-08)	.30 per page			Electronic Recording Authorization Account

ELECTRONIC RECORDING DELIVERY SYSTEM
SECURE ACCESS
DISQUALIFYING OFFENSES

For the purposes of fingerprinting, Secure Access[2] refers to an individual's ability to submit documents for recording in a digitized environment. No person shall be granted secure access to an electronic recording delivery system if he or she has been convicted of a felony, has been convicted of a misdemeanor related to theft, fraud, or a crime of moral turpitude, or if he or she has pending criminal charges for any of these crimes. A plea of guilty or no contest, a verdict resulting in conviction, or the forfeiture of bail, shall be a conviction within the meaning of GC section, 27395 (a), irrespective of a subsequent order under Section 1203.4 of the Penal Code.

A felony conviction or pending charges involving the following offenses will be justification for denial of secure access:

Felony:

• Homicide	• Forgery
• Robbery	• Arson
• Assault	• Drugs
• Kidnapping	• Sex
• Burglary	• Driving under the Influence
• Theft	• Hit and Run
• Motor Vehicle Theft	• Weapons
• Escape	• Bookmaking
• Identity Theft	• Unauthorized Access to Computers

And/Or

Any other state or federal felony convictions including pending charges, involving dishonesty, fraud or deceit, which are substantially related to the qualifications, functions, or duties of a person engaged in the secure access of an electronic recording delivery system as described within Government Code Sections 27390-27399.

A misdemeanor conviction or pending charges involving the following offenses will be justification for denial of secure access:

Misdemeanor:

• Misdemeanor manslaughter	• Liquor Laws
• Assault and Battery	• Disturbing the Peace
• Theft	• Malicious Mischief
• Drugs	• Driving under the Influence
• Sex	• Gambling
• Checks and Access Cards	• Trespassing
• Vandalism	• Contributing to the delinquency of a minor
• Identity Theft	• Unauthorized Access to Computers

And/Or

Any other state or federal felony convictions, including pending charges, involving "moral turpitude" [People v. Castro (1985) 38 Cal. 3d 301], provided that the crimes are substantially related to qualifications, functions, or duties of a person engaged in the secure access of an electronic recording delivery system as described within Government Code Sections 27390-27399. Examples of crimes involving moral turpitude include murder, rape, assault with a deadly weapon, hit-and-run, arson, robbery, burglary, possession of drugs for sale, sale of drugs, pimping and pandering, etc.

[2] The fingerprint requirement does not apply to an individual who has been granted 'authorized access' and who is limited to submitting digital documents only; however, all individuals granted 'Secure Access' or 'Authorized Access' by a County Recorder must sign ERDS 0005, Application Attachment Vendor Employee (s) and/or Business Entity(ies) – Attachment A.

INSERT
AB 578 AND AB 1738 HERE

INSERT REGULATIONS HERE

INSERT BASELINE REQUIREMENTS AND TECHNOLOGY STANDARDS HERE

Forms ERDS Requirements Document

This identifies who has responsibility for the completion of and/or submission of the following forms:

Form Name	Vendor	Computer Security Auditor	County Recorder
ERDS 0001 - Application for System Certification			X
ERDS 0002 - Application for Computer Security Auditor Approval		X	
ERDS 0003 - Application for Vendor of Software Certification	X		
ERDS 0004 - Approval of Computer Security Auditor Employee(s) Attachment A		X	
ERDS 0005 - Application Attachment Vendor Employee(s) and/or Business Entity(ies) Attachment A	X		
ERDS 0006 - Request for Replacement of Certificate or Application Documents	X	X	X
ERDS 0008 - Change of Secure and/or Authorized Access			X
ERDS 0009 - Vendor Application Form for Reference(s) Attachment B	X		
ERDS 0010 - Application for Withdrawal	X	X	X
ERDS 0011 - Secure and Authorized Access Statement			X
BCII 8016 - Request for Live Scan Service	X	X	X
FD-258 - Fingerprint Hard Card	X	X	X